Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Freemaths : Tous droits réservés

Petit théorème de Fermat

03

Correction

NB. Enoncé du petit théorème de Fermat : Si *P* est un nombre premier et si *a* est un entier non divisible par *P*, alors $a^{P-1} \equiv 1 \ \ [P]$.

Rappelons aussi que sont équivalentes les formulations :

- *a* est multiple de *b*.
- *a* est divisible par *b*.
- $a \equiv 0 \ \ [b]$.

Partie A

Dans cette partie, *n* est un entier strictement positif et $a = n^{13} - n$.

1. Montrons que *a* est divisible par 7 et par 13 :

Proposons d'abord deux expressions factorisées de *a* :

- D'abord : $a = n \times (n^{12} - 1)$ en factorisant par *n*.
- Ensuite, $n^{12} - 1$ est une différence de deux carrés. L'identité $x^2 - y^2 = (x - y)(x + y)$ peut s'appliquer avec $\begin{cases} x = n^6 \\ y = 1 \end{cases}$. Nous obtenons la factorisation : $a = n \times (n^6 - 1)(n^6 + 1)$

Montrons que *a* est divisible par 7 :

Nous allons démontrer que, quel que soit l'entier naturel *n*, l'un des deux facteurs *n* ou bien $(n^6 - 1)$ de la deuxième factorisation proposée est divisible par 7.

- 7 est un nombre premier.

Si l'entier *n* est divisible par 7, le nombre $a = n \times (n^6 - 1)(n^6 + 1)$est aussi divisible par 7 puisque son facteur *n* est divisible par 7.

Sinon, nous pouvons appliquer le petit théorème de Fermat avec l'entier *n*, le nombre premier $p = 7$ et $p - 1 = 6$.

D'après le petit théorème de Fermat : $n^6 \equiv 1 \;\; [7]$. Nous en déduisons que $n^6 - 1 \equiv 0 \;\; [7]$ donc que $n^6 - 1$ est divisible par 7. Le nombre $a = n \times (n^6 - 1)(n^6 + 1)$ est aussi divisible par 7 puisque son facteur $(n^6 - 1)$ est divisible par 7.

Donc, dans tous les cas, dans $a = n \times (n^6 - 1)(n^6 + 1)$, l'un des deux facteurs *n* ou bien $(n^6 - 1)$ est divisible par 7.

Quel que soit l'entier strictement positif *n*, *a* est divisible par 7.

Montrons que *a* est divisible par 13 :

Nous allons démontrer que, quel que soit l'entier naturel *n*, l'un des deux facteurs *n* ou bien $(n^{12} - 1)$ de la première factorisation proposée est divisible par 13.

- 13 est un nombre premier.

Si l'entier *n* est divisible par 13, le nombre $a = n \times (n^{12} - 1)$ est aussi divisible par 13 puisque son facteur *n* est divisible par 13.

Sinon, nous pouvons appliquer le petit théorème de Fermat avec l'entier *n*, le nombre premier $p = 13$ et $p - 1 = 12$.

D'après le petit théorème de Fermat : $n^{12} \equiv 1 \;\; [13]$. Nous en déduisons que $n^{12} - 1 \equiv 0 \;\; [13]$ donc que $n^{12} - 1$ est divisible par 13. Le nombre $a = n \times (n^{12} - 1)$est aussi divisible par 13 puisque son facteur $(n^{12} - 1)$ est divisible par 13.

Donc, dans tous les cas, dans $a = n \times (n^{12} - 1)$, l'un des deux facteurs *n* ou bien $(n^{12} - 1)$ est divisible par 13.

Quel que soit l'entier strictement positif *n*, *a* est divisible par 13.

Bilan général :

Quel que soit l'entier strictement positif *n*, *a* est divisible par 7 et par 13.

2. Déduisons-en que *a* est divisible par 182 :

Remarquons que $182 = 2 \times 7 \times 13$. Ainsi, 182 est le produit des trois nombres premiers 2, 7 et 13.

Les entiers 2, 7 et 13 étant des nombres premiers distincts, ils sont premiers entre eux deux à deux. De ce fait, leur PPCM est égal à leur produit. Un entier est divisible par 182 si et seulement s'il est divisible à la fois par 2, par 7 et par 13.

(NB. Le fait que 2, 7 et 13 soient premiers entre eux deux à deux est indispensable pour la justification de cette équivalence).

La question précédente a montré que *a* était divisible par 7 et par 13. Il reste maintenant à justifier que *a* est divisible par 2.

La factorisation $a = n \times (n^{12} - 1)$ montre que :

- Si *n* est pair, *a* l'est aussi.
- Si *n* est impair, le nombre n^{12} l'est aussi et le nombre $(n^{12} - 1)$ est pair. Donc *a* est pair.

L'entier *a* est multiple de 2 quelles que soient les circonstances.

Concluons :

Quel que soit l'entier strictement positif *n*, *a* est à la fois multiple de 2, 7 et 13, il est donc multiple de leur PPCM qui est égal à 182.

Partie B

NB. Curieusement, l'énoncé change les rôles des notations *a* et *n* par rapport à ceux de la partie A. Dont acte … Il conviendra de faire attention à ce que l'on écrit.

Remarquons que $62 = 2 \times 31$.

Les entiers 2 et 31 étant des nombres premiers distincts, ils sont premiers entre eux. De ce fait, leur PPCM est égal à leur produit. Un entier est divisible par 62 si et seulement s'il est divisible à la fois par 2 et par 31.

Cette équivalence s'exprime en langage de congruences ainsi : un entier est congru à 0 modulo 62 si et seulement s'il est congru à 0 à la fois modulo 2 et modulo 31.

(L'hypothèse « 2 et 31 sont premiers entre eux » est indispensable pour la justification de cette équivalence).

1. Montrons que $\boldsymbol{a^{31} - a \equiv 0\ [62]}$:

Posons $b = a^{31} - a$. Nous allons utiliser la factorisation : $b = a \times (a^{30} - 1)$.

Montrons que *b* est un nombre pair :

- Si *a* est pair, alors *b* est pair en tant que multiple de *a*.
- Si *a* est impair, toutes ses puissances entières positives sont impaires, en particulier sa puissance trentième et $(a^{30} - 1)$ est un nombre pair. Alors *b* est pair en tant que multiple du nombre pair $(a^{30} - 1)$.

Quelles que soient les circonstances, *b* est pair (en langage de congruences : $b \equiv 0\ [2]$).

Montrons que *b* est divisible par 31 :

- Le nombre 31 est un nombre premier.

Si *a* est un multiple de 31, alors $b = a \times (a^{30} - 1)$ est un multiple de 31 en tant que multiple de *a*.

Sinon, nous pouvons appliquer le petit théorème de Fermat avec l'entier *a*, le nombre premier $p = 31$ et $p - 1 = 30$.

D'après le petit théorème de Fermat : $a^{30} \equiv 1\ [31]$. Nous en déduisons que $a^{30} - 1 \equiv 0\ [31]$ donc que $a^{30} - 1$ est divisible par 31. Le nombre $b = a \times (a^{30} - 1)$est aussi divisible par 31 puisque son facteur $(a^{30} - 1)$ est divisible par 31.

Donc, dans tous les cas, dans $b = a \times (a^{30} - 1)$, l'un des deux facteurs *a* ou bien $(a^{30} - 1)$ est divisible par 31.

Quel que soit l'entier naturel *a*, *b* est divisible par 31 (en langage de congruences : $b \equiv 0\ [31]$).

Bilan général :

Quel que soit l'entier naturel *a*, *b* est divisible à la fois par 2 et par 31, il est donc divisible par leur PPCM qui est égal à 62.

En langage de congruences, puisque $b \equiv 0\ [2]$) et $b \equiv 0\ [31]$:

$b = a^{31} - a \equiv 0\ [62]$.

Freemaths : Tous droits réservés

2. Montrons que $a^{30+n} - a^n \equiv 0\ [62]$:

Dans cette question, *a* est un entier naturel quelconque et *n* est un entier strictement positif. (Cette question généralise la précédente).

Posons $b_n = a^{30+n} - a^n$ et utilisons la factorisation : $b_n = a^{n-1} \times a \times (a^{30} - 1)$.

Cette factorisation fait entrer en jeu l'entier *b* qui a été étudié dans la question précédente.

Nous avons en effet : $b_n = a^{n-1} \times b$.

L'entier *n* étant supposé strictement positif, l'exposant $n - 1$ est un entier naturel et a^{n-1} est un nombre entier. Par conséquent, b_n est toujours un multiple entier de *b*.

Or, la question 1 a démontré que, quel que soit l'entier naturel *a*, *b* est divisible par 62. Tous ses multiples sont de ce fait eux aussi divisibles par 62. Il en est ainsi, en particulier, de b_n.

Quels que soient l'entier naturel *a* et l'entier strictement positif *n*, b_n est divisible par 62.

En langage de congruences, $b_n = a^{30+n} - a^n \equiv 0\ [62]$.